AMC Pamphlet 25-36

Information Management:

Obtaining a Headquarters, U.S. Army Materiel Command (HQ AMC) Local Area Network Account and Workstation

U.S. Army Materiel Command
9301 Chapek Road
Fort Belvoir, VA 22060-5527
24 February 2007

UNCLASSIFIED

SUMMARY of CHANGE

AMC-P 25-36
Information Management

The changes to AMC-P 25-36 are administrative in nature (i.e., new physical address of Headquarters AMC). There is no substantive change in content.

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
9301 CHAPEK ROAD, FORT BELVOIR, VIRGINIA 22060-5527

AMC PAMPHLET NO. 25-36

24 February 2007

Information Management

OBTAINING A HEADQUARTERS, U.S. ARMY MATERIEL COMMAND (HQ AMC) LOCAL AREA NETWORK ACCOUNT AND WORKSTATION

1. **Purpose.** This pamphlet will provide guidance, define responsibilities, and document the steps required to facilitate obtaining a Workstation and Local Area Network (LAN) Account at Headquarters, U.S. Army Materiel Command (HQ AMC).

2. **Scope.** This pamphlet has been developed to support HQ AMC personnel, to include Department of the Army Civilian employees, United States Military Personnel, HQ AMC Interns, HQ AMC Contractors, and Foreign Representatives working at the Army Materiel Command Headquarters facility, located on Fort Belvoir, Virginia. At the time of publication, the DOIM personnel (DOIM COTR, DOIM IAM) are occupying the positions as identified within this AMC Pamphlet may be contacted utilizing the following e-mail address: amcio-i@hqamc-exchg.army.mil.

3. **References.** Army Regulation (AR) 25-2, Information Assurance, chapter 4, section V: Personnel Security Standards.

---

*This version supersedes AMC-P 25-36, 12 May 04

a. Army Regulation 380-67, Personnel Security Program.

b. DOD Information Technology.

c. AMC Control and Routing Slip, AMC Form 356-R-E.

d. Application for Department of Defense Common Access Card DEERS E, DD Form 1172-2.

The proponent of this regulation is the Chief Information Officer/G-6, Headquarters, U.S. Army Materiel Command. Users are invited to send comments and suggestions for improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, U.S. Army Materiel Command, ATTN: AMCIO-P, 9301 Chapek Road, Fort Belvoir, VA 22060-5527.

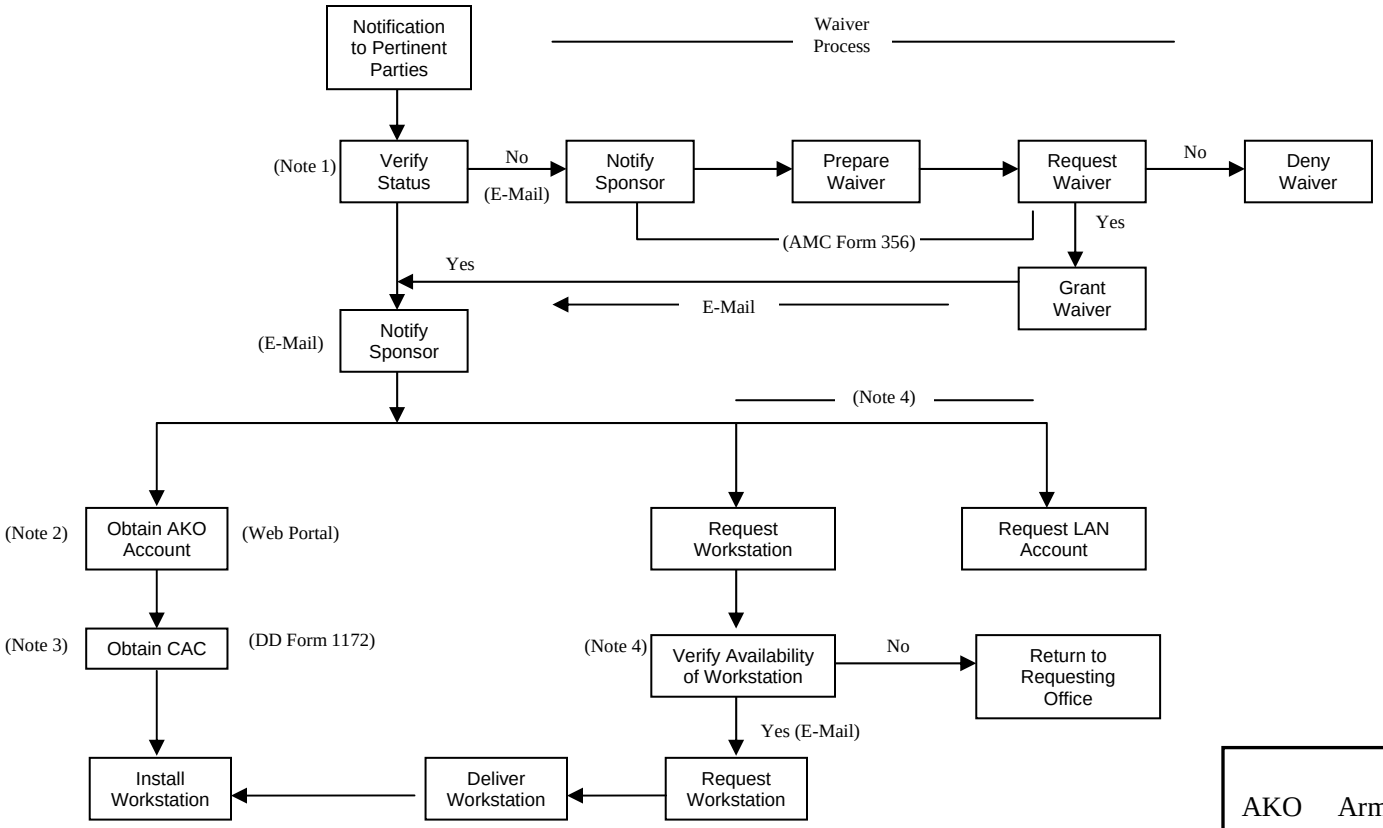
FOR THE COMMANDER:

//Signed//
WILLIAM E. MORTENSEN
Lieutenant General, USA
Chief of Staff

DISTRIBUTION:
B
H

APPENDIX A
Work Flow Diagram

Obtaining an HQ AMC LAN Account and Workstation



Note 1: Status – **Clearance Types**: Top Secret, Secret, Interim
Checks: NAC, NACI** Contractor Hire will have clearance identified as VAL
Note 2: New Hire must identify AMC Sponsor, AMC Sponsor must approve AKO Account Request
New Hire will require AKO Account for CAC
Note 3: AMC Sponsor must complete sec. 3 of DD Form 1172 for Gov't Hire/Intern
New Hire will require CAC to complete PKI Setup for Workstation
**Contractor New Hire must obtain Signature from COR
Note 4: Review/verify/approves Workstation availability against Seat Management Contract

LEGEND

AKO	Army Knowledge Online
AMC	Army Materiel Command
CAC	Command Access Card
COR	Contracting Officer's Representative
NAC	National Agency Check
NACI	National Agency Check w/Inquiries
PKI	Public Key Infrastructure
VAL	Visit Authorization Letter

APPENDIX B
Government/Intern New Hire

Step 1. The AMC CPAC notifies staff section of New Hire. The AMC CPAC (G-1/G-4, Personnel) provides Status of Personnel Security Investigation to Staff section.

Status of Personnel Security Investigation: Completed Personnel Security Investigation: no additional work is required, proceed with Step 2. If no suitable investigation results exist, process required Request for Waiver. (see appendix E, Waiver Process)

Step 2. The staff section notifies (via e-mail, digitally signed) all associated offices of New Hire. (see appendix F, Notification to Pertinent Parties)

Staff section AMC Sponsor
Staff section IT POC/IASO
DOIM COTR

Step 3. The staff section AMC Sponsor identifies requirements for workstation/laptop, to include nonstandard software. (see appendix F, Request for New Seat)

Step 4. New Hire must obtain or have an AKO account. Preferred format is: fname.lname@us.army.mil. Access to the AKO Web Portal will be provided by the staff section AMC Sponsor. The staff section AMC Sponsor may be required to sponsor a New Hire AKO Account. No HQ AMC LAN account can be established without a pre-existing AKO account.

Step 5. The New Hire completes request for Common Access Card (CAC), DD Form 1172, Section 1. The AMC in-line Approving Official Supervisor must sign and complete Section 3 to sponsor the New Hire. The New Hire is responsible for obtaining a CAC from the Military Personnel ID Card Office (DD Form 1172-2 http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage2479.html). A CAC is required for login to the HQ AMC LAN.

Step 6. The staff section IT POC/IASO requests the creation of a LAN Account for New Hire from the Directorate of Information Management (DOIM) IT POC/IASO. Request for New Seat will be submitted via Unicenter ServicePlus Service Desk with Request for New Seat attached. (see appendix F, Request for New Seat)

Step 7. The DOIM COTR reviews/verifies/approves/submits a request (ticket) to Seat Management of new Workstation Requirement. Requests for Workstation that are denied will be returned to the staff section AMC Sponsor and staff section IT POC/IASO. The IASO signs Password Receipt Document (see appendix F, Password Receipt Document) and the new user signs it. User and IASO also sign a copy of the Information Assurance Awareness Policy Overview. (see appendix F, Information Assurance Awareness Policy Overview)

Step 8. Seat Management delivers and deploys new workstation to New Hire. Deployment will require user's signed copy of the Password Receipt Document and CAC to complete PKI and HQ AMC LAN account setup. A CAC is to be provided by the New Hire with a Personal Identification Number (PIN). Seat Management at time of deployment will PKI enable New Hire on assigned workstation.

APPENDIX C
Contractor New Hire

Step 1. The Company notifies Staff section of a new contractor hire. The contractor's employer must submit a Visitor Authorization Letter (VAL) to the staff section. The VAL identifies the clearance status of the New Contractor Hire.

Status of Clearance: Valid Clearance: no additional work is required, proceed with Step 2. If no suitable clearance exists, process required Request for Waiver. (see appendix E, Waiver Process)

Step 2. The staff section notifies all associated offices of New Hire. (see appendix F, Notification to Pertinent Parties) staff section AMC Sponsor (Gov't & Contractor Lead) Staff section IT POC/IASO DOIM COTR

Step 3. The staff section AMC Sponsor/Workload Manager identifies to DOIM IT POC/IASO, requirements for workstation/laptop, to include nonstandard software (Microsoft Project, Microsoft VISIO, etc.). Request for Equipment is to be submitted, via e-mail, digitally signed. (see appendix F, Request for New Seat)

Step 4. The New Contractor Hire must obtain or have an AKO account. Preferred format is: fname.lname@us.army.mil. Access to AKO Web Portal will be provided by staff section AMC Sponsor.

Step 5. The New Contractor Hire completes request for Common Access Card (CAC), DD Form 1172, and Section 1. AMC Contracting Officer's Representative (COR) must sign and complete Section 3 to sponsor New Hire. New Contractor Hire is responsible for obtaining CAC from Military Personnel ID Card Office. (DD Form 1172-2 http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage2479.html). CAC card is required to log into the HQ AMC LAN.

Step 6. DOIM IT POC/IASO based upon requirements submitted by the AMC Sponsor and on behalf of a New Hire, submits an issue for a New Seat using the Unicenter ServicePlus Service Desk and attaches the required template). (see appendix F, Request for New Seat)

Step 7. The DOIM COTR reviews/verifies/approves/submits a request (ticket) to seat management for new workstation requirement. Requests for workstation that are denied are returned to the AMC Sponsor and IT POC/IASO.

Step 8. The IASO signs the password receipt document (see appendix F, Password Receipt Document) and has new user sign it as well. The User and IASO also sign a copy of the Information Assurance Awareness Policy Overview. (see appendix F, Information Assurance Awareness Policy Overview)

Step 9. The seat management delivers and deploys new workstation to new contractor hire. Deployment will require a signed copy of the Password Receipt Document and CAC to complete PKI Set-up. A CAC is to be provided by new contractor hire with Personal Identification Number (PIN). Seat Management, at the time of deployment, will PKI-enable new contractor hire on assigned workstation.

APPENDIX D
Foreign Representative Placement

Step 1. Personnel notify staff section of new Foreign Liaison Officer (LNO). The AMC CPAC provides Status of Personnel Security Investigation to staff section.

Status of Personnel Security Investigation: Completed Personnel Security Investigation: no additional work required, proceed with Step 2. If no suitable investigation results exist, process required Request for Waiver. (see appendix E, Waiver Process)

Step 2. G-Staff notifies all associated offices of new LNO. (see appendix F, Notification to Pertinent Parties)

Step 3. The AMC Sponsor (i.e., the LNO's Contact Officer (CO)) identifies to IT POC/IASO the requirements for workstation/laptop, to include nonstandard software. (see appendix F, Request for New Seat)

Step 4. The new LNO must obtain or have a NIPRNET e-mail account. Format for e-mail address must be: lname.fname.MI.Foreign National.country name.program.host name.army.mil. In order to provide access to AKO, an exception to policy must be generated through G-6 channels to DA G-6 (DISC4) per AR 25-2. Format for e-mail address will be the same as above, except "host name" will be "us." The AKO account must be sponsored. The sponsor should be the LNO's CO.

Step 5. The new LNO completes a request for a Common Access Card (CAC), DD Form 1172 http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage340.html, section 1. AMC in line Approving Official Supervisor must sign and complete Section 3 to sponsor new LNO. (DD Form 1172-2 http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage2479.html)

Step 6. The DOIM IT POC/IASO based upon requirements submitted by AMC Sponsor on behalf of New Hire submits an issue for a New Seat using the Unicenter ServicePlus Service Desk and attaches the required template. (see appendix F, Request for New Seat)

Step 7. The DOIM COTR reviews/verifies/approves/submits a request (ticket) to Seat Management for new workstation requirement. Requests for Workstation that are denied are returned to the AMC Sponsor and IT POC/IASO.

Step 8. The IASO signs Password Receipt Document (see appendix F, Password Receipt Document) and has new user sign it. User and IASO also sign a copy of the Information Assurance Awareness Policy Overview. (see appendix F, Information Assurance Awareness Policy Overview)

Step 9. Seat Management delivers and deploys new workstation to new contractor hire. Deployment will require a signed copy of the Password Receipt Document and CAC to complete PKI Set-up. A CAC is to be provided by new contractor hire with Personal Identification Number (PIN). Seat Management, at the time of deployment, will PKI-enable new contractor hire on assigned workstation.

APPENDIX E
Waiver Process

Under the condition that the New Hire (Government/Intern/Contractor) does not have a valid or suitable clearance, a waiver must be requested in accordance with AR-25-2, Information Assurance, citation 4-16: Personnel Security Standards, and DOD Information Technology Security Accreditation Process (DITSCAP 5200.40, citation appendix E, pg 11-14. To determine clearance level, refer to appendix H, Determining Position Sensitivity and IT Position Designations, of this pamphlet.

Valid Clearance Types:
- Top Secret
- Secret
- Interim

Background Checks:
- NAC/NACI
- Favorable Position of Trust (IT-III Only)

Step 1. The staff section notifies (e-mail, digitally signed) staff section AMC Sponsor and DOIM IT POC/IASO of the Status of Security Clearance and the requirement for a Waiver.

Step 2. The staff section IT POC/IASO prepares a Waiver Request utilizing AMC Form 356 and submits a completed request to DOIM IAM. (AMC Form 356, AMC Control and Routing Slip, http://www.amc.army.mil/amc/ci/pubs/amcform35611.doc). The Request for Waiver must include:

Full Name: (last, first mi)
Company:
Duration of Waiver:
Status of Security Investigation:
System to which Access will be granted:
Justification of Waiver:

Step 3. The DOIM IAM submits Waiver Request to HQ AMC DAA.

Step 4. The HQ-AMC DAA returns Waiver Request (AMC Form 356 http://www.amc.army.mil/amc/ci/pubs/amcform35611.doc) to DOIM IAM.
If the waiver is granted, return to In Process Step 2.
If the waiver is denied, access to HQ AMC Networks or LAN Account is not authorized.

APPENDIX F
Sample Templates

Notification to Pertinent Parties

To be completed by G-Staff and e-mailed to appropriate offices/officers.

Identification	Last Name	First Name
Company/Country Name:	N/A for Government	
Scheduled Arrival Date		
Proposed Division:		
Seat Location/Cubical		

Staff section or Separate Office must notify appropriate office(s). Officials in each office may be different depending on originating office. Offices for G-6 are as follows:

G-Staff IT POC/IASO

DOIM COTR

Note: e-mail correspondence must be digitally signed.

Request for New Seat

AKO Information:
AKO Account Name:
AKO e-mail Address:
CAC (YES/NO):

User Information:
Requested Service Level: (Platinum, Gold, or Silver)
Name (First, Middle, Last):
Title/Rank:
Status (Government, Military, or Contractor):
- Contractor Name:

Clearance Status:
Office Symbol (ex: G-6/AMCIO):

Phone#:
Cubicle/Office Number (ex: 1-2NW4501):

Account Specific Information:
Unclassified Account (Yes/No):
Classified Account (Yes/No):
TSACS Account (Yes/No): Yes
Mailgroups:
Access to Specific Shared Drives/Folder: ??
Printers: ??

IT Hardware Requirement
New Hardware Required: (Yes/No):
If Yes, indicate Desktop, Laptop, or Hi End Workstation

IT Software Requirement
List any Software Applications required to meet your mission. If an application is not already in use at HQ AMC, please submit a separate issue.
(Examples: MS Project, MS Visio, and Adobe Acrobat Writer)

Additional information:
Is user on the TDA Y/N:

Headquarters, U.S. Army Materiel Command (HQ AMC) Information Assurance Awareness Policy Overview

1. As an employee of the Federal Government and a user of government computer services, computer networks, and software, I understand my responsibilities to observe the policies set forth in AR 25-2, and any applicable HQ AMC Information Assurance (IA) directives.

2. Major policies and procedures include, but are not limited to:

a. Use of government telecommunications constitutes consent to ISS monitoring.

b. Use of government computer services, networks, and software is to be used for official government work.

c. User will process and store information ONLY on an accredited or approved system or workstation. (i.e., approvals include sensitive but unclassified , CONFIDENTIAL, SECRET, TOP SECRET, SPECIAL ACCESS PROGRAM, SENSITIVE COMPARTMENTED INFORMATIION (SCI).)

DO NOT PROCESS CLASSIFIED INFORMATION VIA THE UNCLASSIFIED NETWORK (NIPRNET). ALL CLASSIFIED INFORMATION WILL BE PROCESSED VIA THE CLASSIFIED NETWORK (SIPRNET).

---

d. Protect all passwords and other authentication, identification codes and devices from unauthorized disclosure or release.

e. Know the name of your activity Information Assurance Security Officer (IASO) and HQ AMC DOIM Information Assurance Manager (IAM).

f. If you have questions on information assurance (IA) or you do not understand IA policy/procedural statements, then address your concerns with your IASO or contact the HQ AMC DOIM IAM.

g. Report all IA-related incidents and/or violations to your IASO and the HQ AMC DOIM IAM at 806-8799.

h. Physically protect access to computer services, network, hardware and software from access by unauthorized personnel.

i. Use personally owned hardware and software ONLY with written approval of your supervisor, your IASO, and the HQ AMC DOIM IAM.

j. Obey all software copyright instructions and observe federal copyright laws regarding the proper use and reproduction of software.

k. Identify essential data and software and make backups of this data for contingency planning and disaster recovery processes.

l. Store backup materials in an environmentally and physically secure location.

m. Ensure that you use the appropriate available protective measure for all information systems and networks.

n. Report all lost, missing or stolen hardware and software to your supervisor, IASO and the HQ AMC DOIM IAM.

o. Mark and label all removable media (floppy disk, zip disk, CD cartridge, etc.) to identify the content, classification or sensitivity of the information contained within.

p. Use the appropriate HQ AMC label to mark the highest level of classification or sensitivity your computer or workstation has approval to process.

q. Access the internet only to support official mission requirements and as authorized in paragraph 2-301, subparagraph (a). of the Department of Defense Directive (DODD) 5500.7.R DOD Joint Ethics Regulation (“Use of Federal Resources – Communication Systems”).

r. Establish a homepage on the internet only after approval and accreditation from the HQ AMC DOIM IAM, the Operation Security officer, Legal Counsel, and Public Affairs.

s. Avoid computer games, pornography, chain letters, unofficial business for personal use and other forms of behavior, that are inappropriate and outside the scope of official government missions and functions.

t. Do not use any commercial browser chat facilities or chat programs (e.g., AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger, Trillian, IRC, ICQ, etc.) or file sharing programs (e.g., KAZAA, Gnutella, Morpheus, Napster, etc.) They are prohibited on all DOD computer networks.

u. Encrypting computer files is prohibited, with the exception of e-mail encrypted through use of your CAC.

3. Report all virus incidents immediately to your IASO and seek assistance form the Help Desk (806-9333).

_____ _____ _____ _____

Issue #: IS-1--FY06
CO#: CO-1--FY06

PASSWORD RECEIPT DOCUMENT

IT IS MY UNDERSTANDING AS INFORMATION ASSURANCE SECURITY OFFICER (IASO) THAT I WILL COUNSEL THE USER OF THE ACCOUNT DESCRIBED HEREIN ON THE PROPER SECURITY PROCEDURES TO FOLLOW IN ORDER TO PROTECT AND SAFEGUARD THIS ACCOUNT. I WILL INFORM THE USER THAT NO CLASSIFIED INFORMATION IS TO BE PROCESSED ON THE NETWORK AND THAT HE/SHE WILL ENSURE ALL INPUT TO THE NETWORK WILL BE VIRUS-FREE. I WILL INFORM THE USER TO CHANGE THE PASSWORD ON A REGULAR BASIS. I WILL INFORM THE USER THAT THE ACCOUNT IS TO BE USED FOR GOVERNMENT BUSINESS ONLY AND DATA/INFORMATION OR PRODUCTS CREATED USING THIS ACCOUNT REMAIN THE PROPERTY OF THE U. S. GOVERNMENT AND MUST BE SURRENDERED UPON REQUEST. AS IASO, I HAVE VALIDATED THAT THE SUBJECT USER HAS A SATISFACTORILY COMPLETED BACKGROUND INVESTIGATION AND I WILL REPORT ANY MISUSE OF THIS LOG-IN ID AND PASSWORD TO THE HQ AMC INFORMATION ASSURANCE MANAGER (IAM), 2-2SW6006, 806-8799. I ACKNOWLEDGE RECEIPT OF THIS PASSWORD AND WILL IMMEDIATELY PROVIDE IT TO THE USER. I WILL HAVE THE USER REVIEW AND WILL ACKNOWLEDGE HQ AMC AUTOMATED INFORMATION ASSURANCE AWARENESS POLICY OVERVIEW AND RETAIN THIS DOCUMENT ON FILE.

HQ AMC OFFICE: Chief Information Office/G-6

USER NAME: _____ SYSTEM-ID: NT/LOTUS NOTES

OFFICE SYMBOL: AMXxx-x PHONE: 806-XXXX

DATE CO ASSIGNED: XX-XX- 06 LOGIN-ID: AKO.USERNAME

USER JOB TITLE: (Grade/Series)

_____

_____ _____

Information Assurance Manager IASO

DATE ISSUED: XX-XX-06 DATE RECEIVED: XX-XX-06

USER PLEDGE: I WILL COMPLY WITH AND SUPPORT PROVISIONS STIPULATED WITHIN THIS DOCUMENT.

USER SIGNATURE:_____

USER NAME : _____

DATE: _____

COMMENTS:

APPENDIX G
Glossary of Terms

AKO	Army Knowledge Online
AMC	Army Materiel Command
AMC Sponsor	Division Chief of AMC Directorate gaining New Hire
CAC	Common Access Card
CO	Contact Officer
COR	Contracting Officer's Representative
DAA	Designated Approving Authority (AMCIO)
Digitally Signed	PKI Signature, requires CAC
DOIM	Directorate of Information Management
COTR	Contracting Officer's Technical Representative, approving official for new workstation, verifies availability against current Seat Contract
IT POC/IASO	Information Technology Point of Contact/Information Assurance Security Officer
G-Staff	POC within AMC Directorate that receives initial notification from G-1/G-4 of New Hire
HQ AMC DOIM	Headquarters AMC, Directorate of Information Management
IAM	Information Assurance Manager
IASO	Information Assurance Security Officer
IAM	Information Assurance Manager
IT POC	Information Technology Point of Contact
LAN	Local Area Network
LNO	Liaison Officer
NAC	National Agency Check
NACI	National Agency Check with Inquiries
New Hire	New Employee, includes Civilian, Military, Intern, or Contractor
PIN	Personal Identification Number, utilized as a part of PKI
PKI	Public Key Infrastructure
POC	Point of Contact
Seat Management	Contractor supporting HQ AMC with Workstations, LAN, and Help Desk
Workload Manager	Senior POC for New Contractor Hire on site
VAL	Visit Authorization Letter
Web Portal	AKO Web-Page

APPENDIX H
Determining Position Sensitivity and IT Position Designations

1. References:

a. AR 25-2, Information Assurance.

b. AR 380-67, Personnel Security Program.

2. AR 25-2, paragraph 4-14a, identifies the requirement to designate positions requiring access to and processing of information on IT systems. This designation is one determining factor in the type of Personnel Security Investigation that is required. The IT designations are:

a. IT-I. Personnel in these positions have privileged-level access to control, manage, or configure IA tools or devices, PCs, networks, and enclaves. These individuals may be network administrators, system administrators, or directors for information management. An individual assigned to an IT-I position will have their position sensitivity designated as critical sensitive, IAW AR 380-67, and will require the appropriate investigation for a critical sensitive position.

b. IT-II. Personnel in these positions have limited privileged-level access to control, manage, or configure IT tools and devices. These individuals may be back-up operators or system administrators of common applications. Individuals with IT-II duties will be supervised by an individual designated as IT-I. The position sensitivity of an individual performing IT-II duties will be noncritical sensitive. Investigation requirements in AR 380-67 apply.

c. IT-III. All individuals accessing IT systems with non-privileged level access are considered to be performing IT-III duties. These individuals are common users who do not possess system-level access. The position sensitivity for an individual performing IT-III duties will be non-sensitive. Investigation requirements in AR 380-67 also apply.

3. IT designations must not be confused with position sensitivity designations. The IT designation is one determining factor in the investigation process. AR 380-67 requires any individual assigned to a position designated as critical sensitive to submit the appropriate security forms as required to obtain a Top Secret clearance. The same requirement applies to the other two designations: an investigation required to obtain a Secret clearance on any individual assigned to an IT-II and a NAC/NACI for individuals assigned to an IT-III position. If an individual is selected for an IT-I or IT-II position and will not have access to any classified information, the appropriate investigation is still required, although a security clearance need not be provided. Likewise, if an individual is performing IT-III duties, but his/her responsibilities require access to classified information, then the more stringent investigation must take place. Therefore, even though the IT-III designation applies, the position must be designated as either critical sensitive (TS access) or noncritical sensitive (Secret access).